

109TH CONGRESS
1ST SESSION

H. R. 1817

To authorize appropriations for fiscal year 2006 for the Department of Homeland Security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 26, 2005

Mr. COX introduced the following bill; which was referred to the Committee on Homeland Security

A BILL

To authorize appropriations for fiscal year 2006 for the Department of Homeland Security, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Department of Home-

5 land Security Authorization Act for Fiscal Year 2006”.

6 **SEC. 2. TABLE OF CONTENTS.**

7 The table of contents for this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Table of contents.

TITLE I—AUTHORIZATION OF APPROPRIATIONS

- Sec. 101. Department of Homeland Security.
- Sec. 102. Border patrol agents.

- Sec. 103. Departmental management and operations.
- Sec. 104. Critical infrastructure grants.
- Sec. 105. Research and development.
- Sec. 106. Border and transportation security.

TITLE II—TERRORISM PREVENTION, INFORMATION SHARING,
AND RISK ASSESSMENT

Subtitle A—Terrorism Prevention

- Sec. 201. Terrorism Prevention Plan and related budget submission.
- Sec. 202. Consolidated background check process.

Subtitle B—Homeland Security Information Sharing and Analysis
Enhancement

- Sec. 211. Short title.
- Sec. 212. Provision of terrorism-related information to private sector officials.
- Sec. 213. Analytic expertise on the threats from biological agents and nuclear weapons.
- Sec. 214. Alternative analysis of homeland security information.
- Sec. 215. Assignment of information analysis and infrastructure protection functions.
- Sec. 216. Authority for disseminating homeland security-related information.
- Sec. 217. Tom Ridge Homeland Security Fellows Program.
- Sec. 218. Access to nuclear terrorism-related information.
- Sec. 219. Access of Assistant Secretary for Information Analysis to terrorism information.
- Sec. 220. Administration of the Homeland Security Information Network.
- Sec. 221. Homeland Security Advisory System.
- Sec. 222. Use of open source information.
- Sec. 223. Full and efficient use of open source information.

TITLE III—DOMESTIC PREPAREDNESS AND PROTECTION

Subtitle A—Preparedness and Protection

- Sec. 301. National terrorism exercise program.
- Sec. 302. Technology development and transfer.
- Sec. 303. Requirements relating to the Container Security Initiative (CSI).

Subtitle B—Department of Homeland Security Cybersecurity Enhancement

- Sec. 311. Short title.
- Sec. 312. Assistant Secretary for Cybersecurity.
- Sec. 313. Cybersecurity defined.

TITLE IV—MISCELLANEOUS

- Sec. 401. Border security and enforcement coordination and operations.
- Sec. 402. GAO report to Congress.

1 **TITLE I—AUTHORIZATION OF**
2 **APPROPRIATIONS**

3 **SEC. 101. DEPARTMENT OF HOMELAND SECURITY.**

4 There is authorized to be appropriated to the Sec-
5 retary of Homeland Security for the necessary expenses
6 of the Department of Homeland Security for fiscal year
7 2006, \$34,152,143,000.

8 **SEC. 102. BORDER PATROL AGENTS.**

9 Of the amount authorized under section 101, there
10 is authorized to be appropriated for fiscal year 2006 for
11 border security and control between ports of entry, includ-
12 ing for the hiring of 2,000 border patrol agents in addition
13 to the number employed on the date of enactment of this
14 Act, and related training and support costs,
15 \$1,916,427,000.

16 **SEC. 103. DEPARTMENTAL MANAGEMENT AND OPER-**
17 **ATIONS.**

18 Of the amount authorized under section 101, there
19 is authorized to be appropriated for fiscal year 2006 for
20 departmental management and operations, \$634,687,000,
21 of which—

22 (1) \$44,895,000 is authorized for the Depart-
23 ment of Homeland Security Regions Initiative;

24 (2) \$4,459,000 is authorized for Operation In-
25 tegration Staff; and

1 (3) \$56,278,000 is authorized for Office of Se-
2 curity initiatives.

3 **SEC. 104. CRITICAL INFRASTRUCTURE GRANTS.**

4 Of the amount authorized under section 101, there
5 is authorized to be appropriated for fiscal year 2006 for
6 grants and other assistance to improve critical infrastruc-
7 ture protection, \$500,000,000.

8 **SEC. 105. RESEARCH AND DEVELOPMENT.**

9 Of the amount authorized under section 101, there
10 is authorized to be appropriated for fiscal year 2006—

11 (1) \$76,573,000 to support chemical counter-
12 measure development activities of the Directorate of
13 Science and Technology;

14 (2) \$197,314,000 to support a nuclear detec-
15 tion office and related activities of such directorate;

16 (3) \$10,000,000 for research and development
17 of technologies capable of countering threats posed
18 by man-portable air defense systems, including loca-
19 tion-based technologies and non-commercial aircraft-
20 based technologies; and

21 (4) \$10,600,000 for the activities of such direc-
22 torate conducted pursuant to subtitle G of title VIII
23 of the Homeland Security Act of 2002 (6 U.S.C.
24 441 et seq.).

1 **SEC. 106. BORDER AND TRANSPORTATION SECURITY.**

2 Of the amount authorized under section 101, there
3 is authorized to be appropriated for fiscal year 2006—

4 (1) \$826,913,000 for expenses related to
5 Screening Coordination and Operations of the Direc-
6 torate of Border and Transportation Security;

7 (2) \$100,000,000 for weapons of mass destruc-
8 tion detection technology of such directorate; and

9 (3) \$133,800,000 for the Container Security
10 Initiative of such directorate.

11 **TITLE II—TERRORISM PREVEN-**
12 **TION, INFORMATION SHAR-**
13 **ING, AND RISK ASSESSMENT**
14 **Subtitle A—Terrorism Prevention**

15 **SEC. 201. TERRORISM PREVENTION PLAN AND RELATED**
16 **BUDGET SUBMISSION.**

17 (a) DEPARTMENT OF HOMELAND SECURITY TER-
18 RORISM PREVENTION PLAN.—

19 (1) REQUIREMENTS.—Not later than one year
20 after the date of enactment of the Act, and on a reg-
21 ular basis thereafter, the Secretary of Homeland Se-
22 curity shall prepare and submit to the Committee on
23 Homeland Security of the House of Representatives
24 and the Committee on Homeland Security and Gov-
25 ernmental Affairs of the Senate a Department of
26 Homeland Security Terrorism Prevention Plan. The

1 Plan shall be a comprehensive and integrated plan
2 that includes the goals, objectives, milestones, and
3 key initiatives of the Department of Homeland Security
4 to prevent acts of terrorism on the United
5 States, including its territories and interests.

6 (2) CONTENTS.—The Secretary shall include in
7 the Plan the following elements:

8 (A) Identification and prioritization of
9 groups and subgroups that pose the most significant
10 threat of committing acts of terrorism
11 on the United States and its interests.

12 (B) Identification of the most significant
13 current, evolving, and long term terrorist
14 threats to the United States and its interests,
15 including an evaluation of—

16 (i) the materials that may be used to
17 carry out a potential attack;

18 (ii) the methods that may be used to
19 carry out a potential attack; and

20 (iii) the outcome the perpetrators of
21 acts of terrorism aim to achieve.

22 (C) A prioritization of the threats identified
23 under subparagraph (B), based on an assessment
24 of probability and consequence of such
25 attacks.

1 (D) A description of processes and proce-
2 dures that the Secretary shall establish to insti-
3 tutionalize close coordination between the De-
4 partment of Homeland Security and the Na-
5 tional Counter Terrorism Center and other ap-
6 propriate United States intelligence agencies.

7 (E) The policies and procedures the Sec-
8 retary shall establish to ensure the Department
9 gathers real time information from the National
10 Counter Terrorism Center; disseminates this in-
11 formation throughout the Department, as ap-
12 propriate; utilizes this information to support
13 the Department's counter terrorism responsibil-
14 ities; integrates the Department's information
15 collection and analysis functions; and dissemi-
16 nates this information to its operational units,
17 as appropriate.

18 (F) A description of the specific actions
19 the Secretary shall take to identify threats of
20 terrorism on the United States and its inter-
21 ests, and to coordinate activities within the De-
22 partment to prevent acts of terrorism, with spe-
23 cial emphasis on prevention of terrorist access
24 to and use of weapons of mass destruction.

1 (G) A description of initiatives the Sec-
2 retary shall take to share critical terrorism pre-
3 vention information with, and provide terrorism
4 prevention support to, State and local govern-
5 ments and the private sector.

6 (H) A timeline, with goals and milestones,
7 for implementing the Homeland Security Infor-
8 mation Network, the Homeland Security Secure
9 Data Network, and other departmental infor-
10 mation initiatives to prevent acts of terrorism
11 on the United States and its interests, including
12 integration of these initiatives in the operations
13 of the Homeland Security Operations Center.

14 (I) Such other terrorism prevention-related
15 elements as the Secretary considers appro-
16 priate.

17 (3) CONSULTATION.—In formulating the Plan
18 the Secretary shall consult with—

19 (A) the Director of National Intelligence;

20 (B) the Director of the National Counter
21 Terrorism Center;

22 (C) the Attorney General;

23 (D) the Director of the Federal Bureau of
24 Investigation;

25 (E) the Secretary of Defense;

1 (F) the Secretary of State;

2 (G) the Secretary of Energy;

3 (H) the Secretary of the Treasury; and

4 (I) the heads of other Federal agencies and
5 State, county, and local law enforcement agen-
6 cies as the Secretary considers appropriate.

7 (4) CLASSIFICATION.—The Secretary shall pre-
8 pare the Plan in both classified and nonclassified
9 forms.

10 (b) ANNUAL CROSSCUTTING ANALYSIS OF PROPOSED
11 FUNDING FOR DEPARTMENT OF HOMELAND SECURITY
12 PROGRAMS.—

13 (1) REQUIREMENT TO SUBMIT ANALYSIS.—The
14 Secretary of Homeland Security shall submit to the
15 Congress, concurrently with the submission of the
16 President’s budget for each fiscal year, a detailed,
17 crosscutting analysis of the budget proposed for the
18 Department of Homeland Security, by budget func-
19 tion, by agency, and by initiative area, identifying
20 the requested amounts of gross and net appropria-
21 tions or obligational authority and outlays for pro-
22 grams and activities of the Department for each of
23 the following mission areas:

24 (A) To prevent terrorist attacks within the
25 United States.

1 (B) To reduce the vulnerability of the
2 United States to terrorism.

3 (C) To minimize the damage, and assist in
4 the recovery, from terrorist attacks that do
5 occur within the United States.

6 (D) To carry out all functions of the agen-
7 cies and subdivisions within the Department
8 that are not related directly to homeland secu-
9 rity.

10 (2) FUNDING ANALYSIS OF MULTI-PURPOSE
11 FUNCTIONS.—The analysis required under para-
12 graph (1) for functions that are both related directly
13 and not related directly to homeland security shall
14 include a detailed allocation of funding for each spe-
15 cific mission area within those functions, including
16 an allocation of funding among mission support
17 functions, such as agency overhead, capital assets,
18 and human capital.

19 (3) INCLUDED TERRORISM PREVENTION ACTIVI-
20 TIES.—The analysis required under paragraph
21 (1)(A) shall include the following activities (among
22 others) of the Department:

23 (A) Collection and effective use of intel-
24 ligence and law enforcement operations that

1 screen for and target individuals who plan or
2 intend to carry out acts of terrorism.

3 (B) Investigative, intelligence, and law en-
4 forcement operations that identify and disrupt
5 plans for acts of terrorism or reduce the ability
6 of groups or individuals to commit acts of ter-
7 rorism.

8 (C) Investigative activities and intelligence
9 operations to detect and prevent the introduc-
10 tion of weapons of mass destruction into the
11 United States.

12 (D) Initiatives to detect potential, or the
13 early stages of actual, biological, chemical, radi-
14 ological, or nuclear attacks.

15 (E) Screening individuals against terrorist
16 watch lists.

17 (F) Screening cargo to identify and seg-
18 regate high-risk shipments.

19 (G) Specific utilization of information
20 sharing and intelligence, both horizontally
21 (within the Federal Government) and vertically
22 (among Federal, State, and local governments),
23 to detect or prevent acts of terrorism.

24 (H) Initiatives, including law enforcement
25 and intelligence operations, to preempt, disrupt,

1 and deter acts of terrorism overseas intended to
2 strike the United States.

3 (I) Investments in technology, research
4 and development, training, and communications
5 systems that are designed to improve the per-
6 formance of the Department and its agencies
7 with respect to each of the activities listed in
8 subparagraphs (A) through (H).

9 (4) SEPARATE DISPLAYS FOR MANDATORY AND
10 DISCRETIONARY AMOUNTS.—Each analysis under
11 paragraph (1) shall include separate displays for
12 proposed mandatory appropriations and proposed
13 discretionary appropriations.

14 **SEC. 202. CONSOLIDATED BACKGROUND CHECK PROCESS.**

15 (a) REQUIREMENT.—The Secretary shall establish a
16 single process for conducting the security screening and
17 background checks on individuals participating in any vol-
18 untary or mandatory departmental credentialing or reg-
19 istered traveler program.

20 (b) INCLUDED PROGRAMS.—The process established
21 under subsection (a) shall be sufficient to meet the secu-
22 rity requirements of all applicable Departmental pro-
23 grams, including—

24 (1) the Transportation Worker Identification
25 Credential;

- 1 (2) the Hazmat Endorsement Credential;
- 2 (3) the Free and Secure Trade program;
- 3 (4) the NEXUS and SENTRI border crossing
- 4 programs;
- 5 (5) the Registered Traveler program of the
- 6 Transportation Security Administration; and
- 7 (6) any other similar program or credential con-
- 8 sidered appropriate for inclusion by the Secretary.

9 (c) FEATURES OF PROCESS.—The process estab-
10 lished under subsection (a) shall include the following:

11 (1) A single submission of security screening in-
12 formation, including personal data and biometric in-
13 formation as appropriate, necessary to meet the se-
14 curity requirements of all applicable departmental
15 programs.

16 (2) An ability to submit such security screening
17 information at any location or through any process
18 approved by the Secretary with respect to any of the
19 applicable departmental programs.

20 (3) Acceptance by the Department of a security
21 clearance issued by a Federal agency, to the extent
22 that the security clearance process of the agency sat-
23 isfies requirements that are at least as stringent as
24 those of the applicable departmental programs under
25 this section.

1 (4) Standards and procedures for protecting in-
2 dividual privacy, confidentiality, record retention,
3 and addressing other concerns relating to informa-
4 tion security.

5 (d) DEADLINES.—The Secretary of Homeland Secu-
6 rity shall—

7 (1) submit a description of the process devel-
8 oped under subsection (a) to the Committee on
9 Homeland Security of the House of Representatives
10 and the Committee on Homeland Security and Gov-
11 ernmental Affairs of the Senate by not later than 6
12 months after the date of the enactment of this Act;
13 and

14 (2) begin implementing such process by not
15 later than 12 months after the date of the enact-
16 ment of this Act.

17 (e) RELATIONSHIP TO OTHER LAWS.—Nothing in
18 this section affects any statutory requirement relating to
19 the operation of the programs described in subsection (b).

1 **Subtitle B—Homeland Security In-**
2 **formation Sharing and Analysis**
3 **Enhancement**

4 **SEC. 211. SHORT TITLE.**

5 This subtitle may be cited as the “Homeland Security
6 Information Sharing and Analysis Enhancement Act of
7 2005”.

8 **SEC. 212. PROVISION OF TERRORISM-RELATED INFORMA-**
9 **TION TO PRIVATE SECTOR OFFICIALS.**

10 Section 201(d) of the Homeland Security Act of 2002
11 (6 U.S.C. 121(d)) is amended by adding at the end the
12 following:

13 “(20) To require, in consultation with the As-
14 sistant Secretary for Infrastructure Protection, the
15 creation and routine dissemination of analytic re-
16 ports and products designed to provide timely and
17 accurate information that has specific relevance to
18 each of the Nation’s critical infrastructure sectors
19 (as identified in the national infrastructure protec-
20 tion plan issued under paragraph (5)), to private
21 sector officials in each such sector who are respon-
22 sible for protecting institutions within that sector
23 from potential acts of terrorism and for mitigating
24 the potential consequences of any such act.”.

1 **SEC. 213. ANALYTIC EXPERTISE ON THE THREATS FROM BI-**
2 **OLOGICAL AGENTS AND NUCLEAR WEAPONS.**

3 Section 201(d) of the Homeland Security Act of 2002
4 (6 U.S.C. 121(d)) is further amended by adding at the
5 end the following:

6 “(21) To ensure sufficient analytic expertise
7 within the Office of Information Analysis to create
8 and disseminate, on an ongoing basis, products
9 based on the analysis of homeland security informa-
10 tion, as defined in section 892(f)(1), with specific
11 reference to the threat of terrorism involving the use
12 of nuclear weapons and biological agents to inflict
13 mass casualties or other catastrophic consequences
14 on the population or territory of the United States.”.

15 **SEC. 214. ALTERNATIVE ANALYSIS OF HOMELAND SECU-**
16 **RITY INFORMATION.**

17 (a) REQUIREMENT.—Subtitle A of title II of the
18 Homeland Security Act of 2002 (6 U.S.C. 121 et seq.)
19 is amended by adding at the end the following:

20 **“SEC. 203. ALTERNATIVE ANALYSIS OF HOMELAND SECU-**
21 **RITY INFORMATION.**

22 “The Secretary shall establish a process and assign
23 an individual or entity the responsibility to ensure that,
24 as appropriate, elements of the Department conduct alter-
25 native analysis (commonly referred to as ‘red-team anal-
26 ysis’) of homeland security information, as that term is

1 defined in section 892(f)(1), that relates to potential acts
 2 of terrorism involving the use of nuclear weapons or bio-
 3 logical agents to inflict mass casualties or other cata-
 4 strophic consequences on the population or territory of the
 5 United States.”.

6 (b) CLERICAL AMENDMENT.—The table of contents
 7 in section 1(b) of such Act is amended by inserting after
 8 the item relating to section 202 the following:

“Sec. 203. Alternative analysis of homeland security information.”.

9 **SEC. 215. ASSIGNMENT OF INFORMATION ANALYSIS AND**
 10 **INFRASTRUCTURE PROTECTION FUNCTIONS.**

11 Section 201(b) of the Department of Homeland Secu-
 12 rity Act of 2002 (6 U.S.C. 121(b)) is amended by adding
 13 at the end the following:

14 “(4) ASSIGNMENT OF SPECIFIC FUNCTIONS.—
 15 The Under Secretary for Information Analysis and
 16 Infrastructure Protection—

17 “(A) shall assign to the Assistant Sec-
 18 retary for Information Analysis the responsi-
 19 bility for performing the functions described in
 20 paragraphs (1), (3), (4), (7) through (16), and
 21 (18) of subsection (d);

22 “(B) shall assign to the Assistant Sec-
 23 retary for Infrastructure Protection the respon-
 24 sibility for performing the functions described

1 in paragraphs (2), (5), and (6) of subsection
2 (d);

3 “(C) shall ensure that the Assistant Sec-
4 retary for Information Analysis and the Assist-
5 ant Secretary for Infrastructure Protection both
6 perform the functions described in paragraphs
7 (17) and (19) of subsection (d);

8 “(D) may assign to each such Assistant
9 Secretary such other duties relating to such re-
10 sponsibilities as the Under Secretary may pro-
11 vide; and

12 “(E) shall direct each such Assistant Sec-
13 retary to coordinate with elements of the intel-
14 ligence community, with Federal, State, and
15 local law enforcement agencies, and with tribal
16 and private sector entities, as appropriate.”.

17 **SEC. 216. AUTHORITY FOR DISSEMINATING HOMELAND SE-**
18 **CURITY-RELATED INFORMATION.**

19 (a) IN GENERAL.—Title I of the Homeland Security
20 Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding
21 at the end the following:

22 **“SEC. 104. AUTHORITY FOR DISSEMINATING HOMELAND SE-**
23 **CURITY-RELATED INFORMATION.**

24 “(a) PRIMARY AUTHORITY.—Except as provided in
25 subsection (b), the Secretary shall be the executive branch

1 official responsible for disseminating homeland security-
2 related information to State and local government and
3 tribal officials and the private sector.

4 “(b) **PRIOR APPROVAL REQUIRED.**—No Federal offi-
5 cial may issue any homeland security-related analysis, ad-
6 visory, or alert without the Secretary’s prior approval, ex-
7 cept—

8 “(1) in exigent circumstances under which it is
9 essential that the information be communicated im-
10 mediately; or

11 “(2) when such analysis advisory or alert is
12 issued to State, local, or tribal law enforcement offi-
13 cials for the purpose of assisting them in any aspect
14 of the administration of criminal justice.”.

15 (b) **CLERICAL AMENDMENT.**—The table of contents
16 in section 1(b) of such Act is amended by adding at the
17 end the following:

“Sec. 104. Authority for disseminating homeland security-related information.”.

18 **SEC. 217. TOM RIDGE HOMELAND SECURITY FELLOWS PRO-**
19 **GRAM.**

20 (a) **ESTABLISHMENT OF PROGRAM.**—Subtitle A of
21 title II of the Homeland Security Act of 2002 (6 U.S.C.
22 121 et seq.) is further amended by adding at the end the
23 following:

1 **“SEC. 204. TOM RIDGE HOMELAND SECURITY FELLOWS**
2 **PROGRAM.**

3 “(a) ESTABLISHMENT.—

4 “(1) IN GENERAL.—The Secretary shall estab-
5 lish a fellowship program in accordance with this
6 section for the purpose of bringing State, local, trib-
7 al, and private sector officials to participate in the
8 work of the Homeland Security Operations Center in
9 order to become familiar with—

10 “(A) the mission and capabilities of that
11 Center; and

12 “(B) the role, programs, products, and
13 personnel of the Office of Information Analysis
14 and the Office of Infrastructure Protection.

15 “(2) PROGRAM NAME.—The program under
16 this section shall be known as the ‘Tom Ridge
17 Homeland Security Fellows Program’.

18 “(b) ELIGIBILITY.—In order to be eligible for selec-
19 tion as a fellow under the program, an individual must—

20 “(1) have homeland security-related responsibil-
21 ities; and

22 “(2) possess an appropriate national security
23 clearance.

24 “(c) LIMITATIONS.—The Secretary—

1 “(1) may conduct up to 4 iterations of the pro-
2 gram each year, each of which shall be 90 days in
3 duration; and

4 “(2) shall ensure that the number of fellows se-
5 lected for each iteration does not impede the activi-
6 ties of the Center.

7 “(d) CONDITION.—As a condition of selecting an in-
8 dividual as a fellow under the program, the Secretary shall
9 require that the individual’s employer agree to continue
10 to pay the individual’s salary and benefits during the pe-
11 riod of the fellowship.

12 “(e) STIPEND.—During the period of the fellowship
13 of an individual under the program, the Secretary shall,
14 subject to the availability of appropriations—

15 “(1) provide to the individual a stipend to cover
16 the individual’s reasonable living expenses during the
17 period of the fellowship; and

18 “(2) reimburse the individual for round-trip,
19 economy fare travel to and from the individual’s
20 place of residence twice each month.”.

21 (b) CLERICAL AMENDMENT.—The table of contents
22 in section 1(b) of such Act is further amended by adding
23 at the end of the items relating to such subtitle the fol-
24 lowing:

“Sec. 204. Tom Ridge Homeland Security Fellows Program.”.

1 **SEC. 218. ACCESS TO NUCLEAR TERRORISM-RELATED IN-**
2 **FORMATION.**

3 Section 201(d) of the Homeland Security Act of 2002
4 (6 U.S.C. 121(d)) is further amended by adding at the
5 end the following:

6 “(22) To ensure that—

7 “(A) the Assistant Secretary for Informa-
8 tion Analysis receives promptly and without re-
9 quest all information obtained by any compo-
10 nent of the Department if that information re-
11 lates, directly or indirectly, to a threat of ter-
12 rorism involving the potential use of nuclear
13 weapons;

14 “(B) such information is—

15 “(i) integrated and analyzed com-
16 prehensively; and

17 “(ii) disseminated in a timely manner,
18 including to appropriately cleared State,
19 local, tribal, and private sector officials;
20 and

21 “(C) such information is used to determine
22 what requests the Department should submit
23 for collection of additional information relating
24 to that threat.”.

1 **SEC. 219. ACCESS OF ASSISTANT SECRETARY FOR INFOR-**
2 **MATION ANALYSIS TO TERRORISM INFORMA-**
3 **TION.**

4 Section 201(d) of the Homeland Security Act of 2002
5 (6 U.S.C. 121(d)) is further amended by adding at the
6 end the following:

7 “(23) To ensure that the Assistant Secretary
8 for Information Analysis—

9 “(A) is routinely and without request given
10 prompt access to all terrorism-related informa-
11 tion collected by or otherwise in the possession
12 of any component of the Department, including
13 all homeland security information (as that term
14 is as defined in section 892(f)(1)); and

15 “(B) to the extent technologically feasible
16 has direct access to all databases of any compo-
17 nent of the Department that may contain such
18 information.”.

19 **SEC. 220. ADMINISTRATION OF THE HOMELAND SECURITY**
20 **INFORMATION NETWORK.**

21 Section 201(d) of the Homeland Security Act of 2002
22 (6 U.S.C. 121(d)) is further amended by adding at the
23 end the following new paragraph:

24 “(24) To administer the homeland security in-
25 formation network, including—

1 “(A) exercising primary responsibility for
2 creating a secure nationwide real-time home-
3 land security information sharing network for
4 Federal, State, and local government agencies
5 and authorities, tribal officials, the private sec-
6 tor, and other governmental and private entities
7 involved in receiving, analyzing, and distrib-
8 uting information related to threats to home-
9 land security; and

10 “(B) ensuring that the information sharing
11 systems, developed in connection with the net-
12 work created under subparagraph (A), utilize
13 and are compatible with, to the greatest extent
14 practicable, Federal, State, and local govern-
15 ment, tribal, and private sector antiterrorism
16 systems and protocols that have been or are
17 being developed.”.

18 **SEC. 221. HOMELAND SECURITY ADVISORY SYSTEM.**

19 (a) IN GENERAL.—Subtitle A of title II of the Home-
20 land Security Act of 2002 is amended—

21 (1) in section 201(d)(7) 6U.S.C. 121(d)(7)) by
22 inserting “under section 205” after “System”; and

23 (2) by adding at the end the following:

1 **“SEC. 205. HOMELAND SECURITY ADVISORY SYSTEM.**

2 “(a) REQUIREMENT.—The Under Secretary for In-
3 formation Analysis and Infrastructure Protection shall im-
4 plement a Homeland Security Advisory System in accord-
5 ance with this section to provide public advisories and
6 alerts regarding threats to homeland security, including
7 national, regional, local, and economic sector advisories
8 and alerts, as appropriate.

9 “(b) REQUIRED ELEMENTS.—The Under Secretary,
10 under the System—

11 “(1) shall include, in each advisory and alert re-
12 garding a threat, information on appropriate protec-
13 tive measures and countermeasures that may be
14 taken in response to the threat;

15 “(2) shall, whenever possible, limit the scope of
16 each advisory and alert to a specific region, locality,
17 or economic sector believed to be at risk; and

18 “(3) shall not, in issuing any advisory or alert,
19 use color designations as the exclusive means of
20 specifying the homeland security threat conditions
21 that are the subject of the advisory or alert.”.

22 (b) CLERICAL AMENDMENT.—The table of contents
23 in section 1(b) of such Act is amended by adding at the
24 end of the items relating to subtitle A of title II the fol-
25 lowing:

“Sec. 205. Homeland Security Advisory System.”.

1 **SEC. 222. USE OF OPEN SOURCE INFORMATION.**

2 Section 201(d) of the Homeland Security Act of 2002
3 (6 U.S.C. 121(d)) is further amended by adding at the
4 end the following:

5 “(25) To ensure that, whenever possible—

6 “(A) the Assistant Secretary for Informa-
7 tion Analysis produces and disseminates reports
8 and analytic products based on open-source in-
9 formation that do not require a national secu-
10 rity classification under applicable law; and

11 “(B) such unclassified open source reports
12 are produced and disseminated contempora-
13 neously with reports or analytic products con-
14 cerning the same or similar information that
15 the Assistant Secretary for Information Anal-
16 ysis produces and disseminates in a classified
17 format.”.

18 **SEC. 223. FULL AND EFFICIENT USE OF OPEN SOURCE IN-**
19 **FORMATION.**

20 (a) REQUIREMENT.—Subtitle A of title II of the
21 Homeland Security Act of 2002 (6 U.S.C. 121 et seq.)
22 is amended by adding at the end the following:

23 **“SEC. 206. FULL AND EFFICIENT USE OF OPEN SOURCE IN-**
24 **FORMATION.**

25 “The Under Secretary shall ensure that, in meeting
26 their analytic responsibilities under section 201(d) and in

1 formulating requirements for collection of additional infor-
 2 mation, the Assistant Secretary for Information Analysis
 3 and the Assistant Secretary for Infrastructure Protection
 4 make full and efficient use of open-source information.”.

5 (b) CLERICAL AMENDMENT.—The table of contents
 6 in section 1(b) of such Act is amended by inserting after
 7 the item relating to section 202 the following:

“Sec. 206. Full and efficient use of open source information.”.

8 **TITLE III—DOMESTIC PRE-**
 9 **PAREDNESS AND PROTEC-**
 10 **TION**

11 **Subtitle A—Preparedness and**
 12 **Protection**

13 **SEC. 301. NATIONAL TERRORISM EXERCISE PROGRAM.**

14 (a) IN GENERAL.—Section 430 of the Homeland Se-
 15 curity Act of 2002 (6 U.S.C. 238) is amended by striking
 16 “and” after the semicolon at the end of paragraph (8),
 17 by striking the period at the end of paragraph (9) and
 18 inserting “; and”, and by adding at the end the following:

19 “(10) designing, developing, performing, and
 20 evaluating exercises at the National, State, terri-
 21 torial, regional, local, and tribal levels of government
 22 that incorporate government officials, emergency re-
 23 sponse providers, public safety agencies, the private
 24 sector, international governments and organizations,
 25 and other appropriate entities to test the Nation’s

1 capability to prevent, prepare for, respond to, and
2 recover from threatened or actual acts of ter-
3 rorism.”.

4 (b) NATIONAL TERRORISM EXERCISE PROGRAM.—

5 (1) ESTABLISHMENT OF PROGRAM.—Title VIII
6 of the Homeland Security Act of 2002 (Public Law
7 107–296) is amended by adding at the end the fol-
8 lowing new subtitle:

9 **“Subtitle J—Terrorism**
10 **Preparedness Exercises**

11 **“SEC. 899a. NATIONAL TERRORISM EXERCISE PROGRAM.**

12 “(a) IN GENERAL.—The Secretary, through the Of-
13 fice for Domestic Preparedness, shall establish a National
14 Terrorism Exercise Program for the purpose of testing
15 and evaluating the Nation’s capabilities to prevent, pre-
16 pare for, respond to, and recover from threatened or ac-
17 tual acts of terrorism that—

18 “(1) enhances coordination for terrorism pre-
19 paredness between all levels of government, emer-
20 gency response providers, international governments
21 and organizations, and the private sector;

22 “(2) is—

23 “(A) multidisciplinary in nature, including,
24 as appropriate, information analysis and
25 cybersecurity components;

1 “(B) as realistic as practicable and based
2 on current risk assessments, including credible
3 threats, vulnerabilities, and consequences;

4 “(C) carried out with the minimum degree
5 of notice to involved parties regarding the tim-
6 ing and details of such exercises, consistent
7 with safety considerations;

8 “(D) evaluated against performance meas-
9 ures and followed by corrective action to solve
10 identified deficiencies; and

11 “(E) assessed to learn best practices,
12 which shall be shared with appropriate Federal,
13 State, territorial, regional, local, and tribal per-
14 sonnel, authorities, and training institutions for
15 emergency response providers; and

16 “(3) assists State, territorial, local, and tribal
17 governments with the design, implementation, and
18 evaluation of exercises that—

19 “(A) conform to the requirements of para-
20 graph (2); and

21 “(B) are consistent with any applicable
22 State homeland security strategy or plan.

23 “(b) NATIONAL LEVEL EXERCISES.—The Secretary,
24 through the National Terrorism Exercise Program, shall

1 perform on a periodic basis national terrorism prepared-
 2 ness exercises for the purposes of—

3 “(1) involving top officials from Federal, State,
 4 territorial, local, tribal, and international govern-
 5 ments, as the Secretary considers appropriate;

6 “(2) testing and evaluating the Nation’s capa-
 7 bility to detect, disrupt, and prevent threatened or
 8 actual catastrophic acts of terrorism, especially those
 9 involving weapons of mass destruction; and

10 “(3) testing and evaluating the Nation’s readi-
 11 ness to respond to and recover from catastrophic
 12 acts of terrorism, especially those involving weapons
 13 of mass destruction.”.

14 (2) CLERICAL AMENDMENT.—The table of con-
 15 tents in section 1(b) of such Act is amended by add-
 16 ing at the end of the items relating to title VIII the
 17 following:

“Subtitle J—Terrorism Preparedness Exercises

“Sec. 899a. National terrorism exercise program.”.

18 **SEC. 302. TECHNOLOGY DEVELOPMENT AND TRANSFER.**

19 (a) ESTABLISHMENT OF TECHNOLOGY CLEARING-
 20 HOUSE.—Not later than 90 days after the date of enact-
 21 ment of this Act, the Secretary shall complete the estab-
 22 lishment of the Technology Clearinghouse under section
 23 313 of the Homeland Security Act of 2002.

1 (b) TRANSFER PROGRAM.—Section 313 of the Home-
2 land Security Act of 2002 (6 U.S.C. 193) is amended—

3 (1) by adding at the end of subsection (b) the
4 following new paragraph:

5 “(6) The establishment of a homeland security
6 technology transfer program to facilitate the identi-
7 fication, modification, and commercialization of tech-
8 nology and equipment for use by Federal, State, and
9 local governmental agencies, emergency response
10 providers, and the private sector to prevent, prepare
11 for, or respond to acts of terrorism.”;

12 (2) by redesignating subsection (c) as sub-
13 section (d); and

14 (3) by inserting after subsection (b) the fol-
15 lowing new subsection:

16 “(c) TECHNOLOGY TRANSFER PROGRAM.—In devel-
17 oping the program described in subsection (b)(6), the Sec-
18 retary, acting through the Under Secretary for Science
19 and Technology, shall—

20 “(1) in consultation with the other Undersecre-
21 taries of the Department and the Director of the Of-
22 fice for Domestic Preparedness, on an ongoing
23 basis—

24 “(A) conduct surveys and reviews of avail-
25 able appropriate technologies that have been, or

1 are in the process of being developed or dem-
2 onstrated by the Department, other Federal
3 agencies, or the private sector or foreign gov-
4 ernments and international organizations and
5 that may be useful in assisting Federal, State,
6 and local governmental agencies, emergency re-
7 sponse providers, or the private sector to pre-
8 vent, prepare for, or respond to acts of ter-
9 rorism;

10 “(B) conduct or support research and de-
11 velopment as appropriate of technologies identi-
12 fied under subparagraph (A), including any
13 necessary modifications to such technologies for
14 anti-terrorism use;

15 “(C) communicate to Federal, State, and
16 local governmental agencies, emergency re-
17 sponse providers, or the private sector the avail-
18 ability of such technologies for anti-terrorism
19 use, as well as the technology’s specifications,
20 satisfaction of appropriate standards, and the
21 appropriate grants available from the Depart-
22 ment to purchase such technologies;

23 “(D) coordinate the selection and adminis-
24 tration of all technology transfer activities of
25 the Science and Technology Directorate, includ-

1 ing projects and grants awarded to the private
2 sector and academia; and

3 “(E) identify priorities based on current
4 risk assessments within the Department of
5 Homeland Security for identifying, researching,
6 developing, modifying, and fielding existing
7 technologies for anti-terrorism purposes; and

8 “(2) in support of the activities described in
9 paragraph (1)—

10 “(A) consult with Federal, State, and local
11 emergency response providers;

12 “(B) consult with government and nation-
13 ally recognized standards organizations as ap-
14 propriate;

15 “(C) enter into agreements and coordinate
16 with other Federal agencies and foreign govern-
17 ments and international organizations as the
18 Secretary determines appropriate, in order to
19 maximize the effectiveness of such technologies
20 or to facilitate commercialization of such tech-
21 nologies; and

22 “(D) consult with existing technology
23 transfer programs and Federal and State train-
24 ing centers that research, develop, and transfer

1 military and other technologies for use by emer-
2 gency response providers.”.

3 (c) REPORT.—Not later than one year after the date
4 of enactment of this Act, the Under Secretary for Science
5 and Technology shall transmit to the Congress a descrip-
6 tion of the progress the Department has made in imple-
7 menting the provisions of section 313 of the Homeland
8 Security Act of 2002, as amended by this Act, including
9 a description of the process used to review unsolicited pro-
10 posals received as described in subsection (b)(3) of such
11 section.

12 (d) SAVINGS CLAUSE.—Nothing in this section (in-
13 cluding the amendments made by this section) shall be
14 construed to alter or diminish the effect of the limitation
15 on the authority of the Secretary of Homeland Security
16 under section 302(4) of the Homeland Security Act of
17 2002 (6 U.S.C. 182(4)) with respect to human health-re-
18 lated research and development activities.

19 **SEC. 303. REQUIREMENTS RELATING TO THE CONTAINER**
20 **SECURITY INITIATIVE (CSI).**

21 (a) RISK ASSESSMENT AND DESIGNATION OF NEW
22 FOREIGN SEAPORTS.—

23 (1) RISK ASSESSMENT.—The Secretary of
24 Homeland Security shall conduct a risk assessment
25 of each foreign seaport that the Secretary is consid-

1 ering designating as a port under the Container Se-
2 curity Initiative (CSI) on or after the date of the en-
3 actment of this Act. Each such assessment shall
4 evaluate the level of risk for the potential com-
5 promise of cargo containers by terrorists or terrorist
6 weapons at the port.

7 (2) DESIGNATION.—The Secretary is author-
8 ized to designate a foreign seaport as a port under
9 CSI on or after the date of the enactment of this
10 Act only if the Secretary determines pursuant to an
11 assessment under paragraph (1) that a significant
12 level of risk exists for the potential compromise of
13 cargo containers by terrorists or terrorist weapons at
14 the port.

15 (b) DEPLOYMENT OF INSPECTION EQUIPMENT TO
16 NEW CSI PORTS.—

17 (1) DEPLOYMENT.—The Secretary is author-
18 ized to assist in the deployment of non-intrusive in-
19 spection equipment for cargo containers at each CSI
20 port designated under subsection (a)(2) and provide
21 training for personnel at the CSI port to operate the
22 non-intrusive inspection equipment.

23 (2) ADDITIONAL REQUIREMENTS.—The Sec-
24 retary shall establish technical capability require-
25 ments and standard operating procedures for non-in-

1 trusive inspection equipment described in paragraph
2 (1) and shall require each CSI port to agree to oper-
3 ate such equipment in accordance with such require-
4 ments and procedures as a condition for receiving
5 the equipment and training under such paragraph.

6 (c) DEPLOYMENT OF PERSONNEL TO NEW CSI
7 PORTS; RE-EVALUATION OF PERSONNEL AT ALL CSI
8 PORTS.—

9 (1) DEPLOYMENT.—The Secretary shall deploy
10 Department of Homeland Security personnel to each
11 CSI port designated under subsection (a)(1) with re-
12 spect to which the Secretary determines that the de-
13 ployment is necessary to successfully implement the
14 requirements of CSI at the port.

15 (2) RE-EVALUATION.—The Secretary shall peri-
16 odically review relevant risk assessment information
17 with respect to all CSI ports at which Department
18 of Homeland Security personnel are deployed to as-
19 sess whether or not continued deployment of such
20 personnel, in whole or in part, is necessary to suc-
21 cessfully implement the requirements of CSI at the
22 port.

23 (d) INSPECTION AND SCREENING AT UNITED
24 STATES PORTS OF ENTRY.—Cargo containers arriving at
25 a United States port of entry from a CSI port shall under-

1 go the same level of inspection and screening as cargo con-
2 tainers arriving at a United States port of entry from a
3 foreign seaport that is not participating in CSI unless the
4 containers were initially inspected at the CSI port at the
5 request of CSI personnel and such personnel verify and
6 electronically record that the inspection indicates that the
7 containers do not contain unlawful goods or persons.

8 (e) DEFINITION.—In this section, the term “Con-
9 tainer Security Initiative” or “CSI” means the program
10 carried out by the Department of Homeland Security
11 under which the Department enters into agreements with
12 foreign seaports to—

13 (1) establish security criteria to identify high-
14 risk maritime cargo containers bound for the United
15 States based on advance information; and

16 (2) screen or inspect such maritime cargo con-
17 tainers for unlawful goods and persons prior to ship-
18 ment to the United States.

19 **Subtitle B—Department of Home-**
20 **land Security Cybersecurity En-**
21 **hancement**

22 **SEC. 311. SHORT TITLE.**

23 This subtitle may be cited as the “Department of
24 Homeland Security Cybersecurity Enhancement Act of
25 2005”.

1 **SEC. 312. ASSISTANT SECRETARY FOR CYBERSECURITY.**

2 (a) IN GENERAL.—Subtitle A of title II of the Home-
3 land Security Act of 2002 (6 U.S.C. 121 et seq.) is further
4 amended by adding at the end the following:

5 **“SEC. 207. ASSISTANT SECRETARY FOR CYBERSECURITY.**

6 “(a) IN GENERAL.—There shall be in the Directorate
7 for Information Analysis and Infrastructure Protection a
8 National Cybersecurity Office headed by an Assistant Sec-
9 retary for Cybersecurity (in this section referred to as the
10 ‘Assistant Secretary’), who shall assist the Secretary in
11 promoting cybersecurity for the Nation.

12 “(b) GENERAL AUTHORITY.—The Assistant Sec-
13 retary, subject to the direction and control of the Sec-
14 retary, shall have primary authority within the Depart-
15 ment for all cybersecurity-related critical infrastructure
16 protection programs of the Department, including with re-
17 spect to policy formulation and program management.

18 “(c) RESPONSIBILITIES.—The responsibilities of the
19 Assistant Secretary shall include the following:

20 “(1) To establish and manage—

21 “(A) a national cybersecurity response sys-
22 tem that includes the ability to—

23 “(i) analyze the effect of cybersecurity
24 threat information on national critical in-
25 frastructure; and

1 “(ii) aid in the detection and warning
2 of attacks on, and in the restoration of,
3 cybersecurity infrastructure in the after-
4 math of such attacks;

5 “(B) a national cybersecurity threat and
6 vulnerability reduction program that identifies
7 cybersecurity vulnerabilities that would have a
8 national effect on critical infrastructure, per-
9 forms vulnerability assessments on information
10 technologies, and coordinates the mitigation of
11 such vulnerabilities;

12 “(C) a national cybersecurity awareness
13 and training program that promotes
14 cybersecurity awareness among the public and
15 the private sectors and promotes cybersecurity
16 training and education programs;

17 “(D) a government cybersecurity program
18 to coordinate and consult with Federal, State,
19 and local governments to enhance their
20 cybersecurity programs; and

21 “(E) a national security and international
22 cybersecurity cooperation program to help fos-
23 ter Federal efforts to enhance international
24 cybersecurity awareness and cooperation.

1 “(2) To coordinate with the private sector on
2 the program under paragraph (1) as appropriate,
3 and to promote cybersecurity information sharing,
4 vulnerability assessment, and threat warning regard-
5 ing critical infrastructure.

6 “(3) To coordinate with other directorates and
7 offices within the Department on the cybersecurity
8 aspects of their missions.

9 “(4) To coordinate with the Under Secretary
10 for Emergency Preparedness and Response to en-
11 sure that the National Response Plan developed pur-
12 suant to section 502(6) of the Homeland Security
13 Act of 2002 (6 U.S.C. 312(6)) includes appropriate
14 measures for the recovery of the cybersecurity ele-
15 ments of critical infrastructure.

16 “(5) To develop processes for information shar-
17 ing with the private sector, consistent with section
18 214, that—

19 “(A) promote voluntary cybersecurity best
20 practices, standards, and benchmarks that are
21 responsive to rapid technology changes and to
22 the security needs of critical infrastructure; and

23 “(B) consider roles of Federal, State, local,
24 and foreign governments and the private sector,
25 including the insurance industry and auditors.

1 “(6) To coordinate with the Chief Information
2 Officer of the Department in establishing a secure
3 information sharing architecture and information
4 sharing processes, including with respect to the De-
5 partment’s operation centers.

6 “(7) To consult with the Electronic Crimes
7 Task Force of the United States Secret Service on
8 private sector outreach and information activities.

9 “(8) To consult with the Office for Domestic
10 Preparedness to ensure that realistic cybersecurity
11 scenarios are incorporated into tabletop and recovery
12 exercises.

13 “(9) To consult and coordinate, as appropriate,
14 with other Federal agencies on cybersecurity-related
15 programs, policies, and operations.

16 “(10) To consult and coordinate within the De-
17 partment and, where appropriate, with other rel-
18 evant Federal agencies, on security of digital control
19 systems, such as Supervisory Control and Data Ac-
20 quisition (SCADA) systems.

21 “(d) AUTHORITY OVER THE NATIONAL COMMUNICA-
22 TIONS SYSTEM.—The Assistant Secretary shall have pri-
23 mary authority within the Department over the National
24 Communications System.”.

1 (b) CLERICAL AMENDMENT.—The table of contents
2 in section 1(b) of such Act is amended by adding at the
3 end of the items relating to subtitle A of title II the fol-
4 lowing:

“207. Assistant Secretary for Cybersecurity.”.

5 **SEC. 313. CYBERSECURITY DEFINED.**

6 Section 2 of the Homeland Security Act of 2002 (6
7 U.S.C. 101) is amended by adding at the end the fol-
8 lowing:

9 “(17)(A) The term ‘cybersecurity’ means the
10 prevention of damage to, the protection of, and the
11 restoration of computers, electronic communications
12 systems, electronic communication services, wire
13 communication, and electronic communication, in-
14 cluding information contained therein, to ensure its
15 availability, integrity, authentication, confidentiality,
16 and nonrepudiation.

17 “(B) In this paragraph—

18 “(i) each of the terms ‘damage’ and ‘com-
19 puter’ has the meaning that term has in section
20 1030 of title 18, United States Code; and

21 “(ii) each of the terms ‘electronic commu-
22 nications system’, ‘electronic communication
23 service’, ‘wire communication’, and ‘electronic
24 communication’ has the meaning that term has

1 in section 2510 of title 18, United States
2 Code.”.

3 **TITLE IV—MISCELLANEOUS**

4 **SEC. 401. BORDER SECURITY AND ENFORCEMENT COORDI-** 5 **NATION AND OPERATIONS.**

6 (a) FINDINGS.—The Congress makes the following
7 findings:

8 (1) In creating the Department of Homeland
9 Security, the Congress sought to enhance the Na-
10 tion’s capabilities to prevent, protect against, and re-
11 spond to terrorist acts by consolidating existing Fed-
12 eral agencies with homeland security functions into
13 a single new Department, and by realigning the mis-
14 sions of those legacy agencies to more directly sup-
15 port our national homeland security efforts.

16 (2) As part of this massive government reorga-
17 nization, section 442 of the Homeland Security Act
18 of 2002 (Public Law 107–273) established a Bureau
19 of Border Security and transferred into it all of the
20 functions, programs, personnel, assets, and liabilities
21 pertaining to the following programs: the Border Pa-
22 trol; alien detention and removal; immigration-re-
23 lated intelligence, investigations, and enforcement
24 activities; and immigration inspections at ports of
25 entry.

1 (3) Title IV of the Homeland Security Act of
2 2002 (Public Law 107–273) also transferred to the
3 new Department the United States Customs Service,
4 as a distinct entity within the new Department, to
5 further the Department’s border integrity mission.

6 (4) Utilizing its reorganization authority pro-
7 vided in the Homeland Security Act of 2002, the
8 President submitted a reorganization plan for the
9 Department on January 30, 2003.

10 (5) This plan merged the customs and immigra-
11 tion border inspection and patrol functions, along
12 with agricultural inspections functions, into a new
13 entity called United States Customs and Border
14 Protection.

15 (6) The plan also combined the customs and
16 immigration enforcement agents, as well as the Of-
17 fice of Detention and Removal Operations, the Of-
18 fice of Federal Protective Service, the Office of Fed-
19 eral Air Marshal Service, and the Office of Intel-
20 ligence, into another new entity called United States
21 Immigration and Customs Enforcement.

22 (7) The President’s January 30, 2003, reorga-
23 nization plan did not explain the reasons for sepa-
24 rating immigration inspection and border patrol
25 functions from other immigration-related enforce-

1 ment activities, which was contrary to the single Bu-
2 reau of Border Security as prescribed by the Con-
3 gress in the section 441 of the Homeland Security
4 Act of 2002.

5 (8) Two years after this structure has been in
6 effect, questions remain about whether the Depart-
7 ment has organized itself properly, and is managing
8 its customs and immigration enforcement and border
9 security resources in the most efficient, sensible, and
10 effective manner.

11 (9) The current structure has resulted in less
12 cooperation and information sharing between these
13 two critical functions than is desirable, and has
14 caused operational and administrative difficulties
15 that are hampering efforts to secure our borders and
16 ensure the integrity of our border control system.

17 (10) United States Immigration and Customs
18 Enforcement has faced major budgetary challenges
19 that are, in part, attributable to the inexact division
20 of resources upon the separation of immigration
21 functions. These budget shortfalls have forced
22 United States Immigration and Customs Enforce-
23 ment to impose hiring freezes and to release aliens
24 that otherwise should be detained.

1 (11) The current structure also has resulted in
2 unnecessary overlap and duplication between United
3 States Immigration and Customs Enforcement and
4 United States Customs and Border Protection, both
5 in the field and at the headquarters level. There are
6 intelligence, legislative affairs, public affairs and
7 international affairs offices in both agencies.

8 (12) Border security and customs and immigra-
9 tion enforcement should be one seamless mission, fo-
10 cused on ensuring the integrity of our border control
11 system.

12 (b) REPORT.—

13 (1) IN GENERAL.—Not later than 30 days after
14 the date of the enactment of this Act, the Secretary
15 of Homeland Security shall review and evaluate the
16 current organizational structure of the Department
17 of Homeland Security established by the President’s
18 January 30, 2003, reorganization plan and submit a
19 report of findings and recommendations to the Com-
20 mittee on Homeland Security of the House of Rep-
21 resentatives and the Committee on Homeland Secu-
22 rity and Government Affairs of the Senate.

23 (2) CONTENTS OF REPORT.—The report shall
24 include—

1 (A) a description of the rationale for, and
2 any benefits of, the current organizational divi-
3 sion of United States Immigration and Customs
4 Enforcement and United States Customs and
5 Border Protection, with respect to the Depart-
6 ment's homeland security mission;

7 (B) a description of the organization, mis-
8 sions, operations, and policies of United States
9 Customs and Border Protection and United
10 States Immigration and Customs Enforcement,
11 and areas of unnecessary overlap or operational
12 gaps among and between these missions;

13 (C) an analysis of alternative organiza-
14 tional structures that could provide a more ef-
15 fective way to deliver maximum efficiencies and
16 mission success;

17 (D) a description of the current role of the
18 Directorate of Border and Transportation Secu-
19 rity with respect to providing adequate direction
20 and oversight of the two agencies, and whether
21 this management structure is still necessary;

22 (E) an analysis of whether the Federal Air
23 Marshals and the Federal Protective Service are
24 properly located within United States Immigra-
25 tion and Customs Enforcement;

1 (F) the proper placement and functions of
2 a specialized investigative and patrol unit oper-
3 ating at the southwest border on the Tohono
4 O’Odham Nation, known as the Shadow
5 Wolves;

6 (G) the potential costs of reorganization,
7 including financial, programmatic and other
8 costs, to the Department; and

9 (H) a detailed action plan for correcting
10 the operational and administrative problems
11 that have been caused by the division of United
12 States Customs and Border Protection and
13 United States Immigration and Customs En-
14 forcement, including appropriate reorganization
15 plans.

16 **SEC. 402. GAO REPORT TO CONGRESS.**

17 Not later than 6 months after the date of the enact-
18 ment of this Act, the Comptroller General of the United
19 States shall submit to the Congress a report that sets
20 forth—

21 (1) an assessment of the effectiveness of the or-
22 ganizational and management structure of the De-
23 partment of Homeland Security in meeting the De-
24 partment’s counter-terrorism missions; and

1 (2) recommendations to facilitate and improve
2 the organization and management of the Depart-
3 ment to best meet those missions.

○